МЕРЫ ДОВЕРИЯ И ПРАВДОПОДОБИЯ ПРИ ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Волкова Е.С.[1]., Гисин В.Б.[2]

Цель исследования: *разработка методов оценки рисков информационной безопасности в условиях неопределенности, описание механизма распространения доверия и правдоподобия по графу атак.*

Методы исследования: *применение техники мягких вычислений, включая комбинирование свидетельств Демпстера-Шефера, интегрирование по неаддитивным мерам.*

Полученный результат: *разработаны методы оценки рисков и методы оценки ожидаемых потерь в случае, когда факторы риска характеризуются высокой неопределенностью и не позволяют с достаточным обоснованием применить объективные, в частности, вероятностные методы оценки. Исходной информацией служат верхняя и нижняя оценки вероятности реализации риска. С использованием методов теории свидетельств Демпстера-Шефера на графе атак строятся меры доверия и правдоподобия. Описан подход, позволяющий построить меры доверия и правдоподобия в пространстве сценариев атак на основе вероятностных оценок типовых событий информационной безопасности. Показано, как ожидаемый ущерб может быть оценен математическим ожиданием ущерба относительно этих мер с использованием интеграла Шоке.*

Научная новизна: *разработан метод распространения доверия по графу атак. Основой метода служит оригинальный подход к оценке логических комбинаций свидетельств, заданных на бинарных фреймах и представленных дизъюнктивными нормальными формами.*

Ключевые слова: *риск, мера доверия, мера правдоподобия, интеграл Шоке, теория свидетельств.*

DOI:10/21681/2311-3456-2023-1-28-40

Введение

Информационные технологии и коммуникационные устройства все чаще интегрируются в современные системы управления [1, 2]. Переход систем управления на коммуникационные технологии с использованием открытых протоколов (например, TCP/IP, Ethernet) с одной стороны облегчил разработку и развертывание систем и позволил осуществлять дистанционное управление и надзор за инфраструктурой и, тем самым, повысил эффективность. С другой стороны, общая инфраструктура стала более уязвимой для внешних атак.

В публикациях многие авторы [3-5] выражали обеспокоенность по поводу новых угроз, связанных с безопасностью. Интеграция программных компонентов в контуры управления требует решения возникающих проблем безопасности, поскольку злоумышленники используют уязвимости программного обеспечения, связанные с этими архитектурами. В последние годы наблюдается постоянное увеличение как частоты, так и серьезности кибератак. Например, по данным Positive Technologies в III квартале 2022 года количество кибератак по сравнению с аналогичным периодом 2021 года увеличилось на треть, а относительно II квартала — на 10%[3].

Оценка рисков является одной из наиболее важных частей процесса управления рисками, поскольку она служит основой для принятия решений [6]. В соответствии с ГОСТ Р ИСО/МЭК 27001-2021 анализ рисков ИБ является важным компонентом управления рисками. Анализ рисков включает в себя оценку вероятности реализации рисков и потенциальных последствий. Адекватная оценка рисков обеспечивает выбор эффективных мер защиты.

Как отмечается в [7], процессы цифровизации ведут к принципиальному усложнению систем. Безусловно, доминирующими при оценке рисков ИБ в сложных

3 Positive Technologies https://www.ptsecurity.com/ru-ru/ (последнее обращение 22.01.2023)

1 Волкова Елена Сергеевна, кандидат физико-математических наук, доцент Финансового университета при Правительстве Российской Федерации, Москва, Россия. E-mail: evolkova@fa.ru

2 Гисин Владимир Борисович, кандидат физико-математических наук, профессор Финансового университета при Правительстве Российской Федерации, Москва, Россия. E-mail: vgisin@fa.ru

системах остаются традиционные вероятностные методы. Однако иногда применение вероятностных методов выглядит недостаточно обоснованным. Как правило, это связано с тем, что некоторые факторы риска характеризуются высокой неопределенностью и не позволяют с достаточным обоснованием применить объективные, в частности, вероятностные методы оценки (см. [8]). Классическая вероятность требует очень высокого уровня точности и непротиворечивости информации, и поэтому она часто слишком ограничительна, чтобы справляться с многомерной природой неопределенности. Для получения интегрированной картины подверженности рискам информационной безопасности сложных систем используются различные подходы, в том числе так называемые «мягкие» (soft) методы. В общем, мягкие методы получаются за счет ослабления (смягчения) условий в моделях, основанных на стандартных теоретико-вероятностных требованиях.

Одно из все более популярных и успешно применяемых обобщений связано с использованием нижней и верхней вероятностей[4] (см. [9 – 11]), в том числе и при оценке рисков информационной безопасности [12, 13]. Применение нижней и верхней вероятности позволяет обрабатывать информацию без введения неоправданных допущений, что имеет большое значение при оценке рисков и безопасности.

Пусть A — некоторое событие, а $P_{low}(A)$ и $P_{up}(A)$ — соответственно нижняя и верхняя вероятности (оценки вероятности события), так что $0 \le P_{low}(A) \le P_{up}(A) \le 1$. Если значения $P_{low}(A)$ и $P_{up}(A)$ совпадают, их общее значение дает оценку точной вероятности события. Равенства $P_{low}(A) = 0$ и $P_{up}(A) = 1$ означают, что информация о событии отсутствует. В общем случае промежуток $[P_{low}(A), P_{up}(A)]$ дает интервальную оценку вероятности события. Математически эквивалентный подход можно получить, оценивая по отдельности доводы в пользу того, что событие A произойдет или не произойдет. Пусть $P_{yes}(A)$ — оценка первой величины, а $P_{no}(A)$ — оценка второй. Положим $P_{yes}(A) = P_{low}(A)$ и $P_{no}(A) = P_{up}\left(\overline{A}\right) = 1 - P_{up}(A)$, где через $\overline{A}$ обозначено событие не-A. Тогда, как легко видеть, условие $P_{low}(A) \le P_{up}(A)$ равносильно условию.

$$P_{yes}(A) + P_{no}(A) \le 1.$$

Случай $P_{yes}(A) + P_{no}(A) = 1$ соответствует полной информации, случай $P_{yes}(A) + P_{no}(A) = 0$ — отсутствию информации для оценки вероятности события A.

4 Walley P.. Statistical Reasoning with Imprecise Probabilities. – London: Chapman and Hall 1991. 720 p.

Всякая модель оценки рисков, так или иначе, включает в себя описание механизмов принятия решений. Одно из фундаментальных объяснений того, как принимаются решения, принадлежит Сэвиджу. Согласно Сэвиджу, наличие на множестве действий (решений) предпочтений означает, что в пространстве состояний имеется аддитивная вероятностная мера. Проявиться этот результат может в самых разных ситуациях. Например, в [14] в контексте теории Сэвиджа развит теоретико-игровой подход к оценке безопасности сложной сети, применимый к широкому классу систем. Ключевые результаты в конечном итоге основываются на аддитивности функции выигрыша агента, существование которой и обеспечивается теоремой Сэвиджа.

Теория Сэвиджа исходит из того, что субъект, принимающий решения, имеет неискаженные интуитивные представления о вероятностях. Многочисленные исследования в области теории принятия решений, проводившиеся на протяжении многих лет, показывают, что субъективные оценки вероятности зависят от множества факторов и во многих случаях оказываются искаженными (см. [15-17]). Эти искажения, как правило, ведут к нарушению аддитивности. В частности, это имеет место в ситуациях, когда в модель включаются экспертные оценки.

Здесь достаточно адекватными оказываются модели, основанные на использовании неаддитивных мер — так называемых мер доверия. Эти модели получили широкое распространение, особенно в связи с работами в области искусственного интеллекта.

Основа теории мер доверия была заложена работами Демпстера и Шефера (о современном состоянии исследований в этой области см. [18, 19]). В теории свидетельств Демпстера-Шефера вероятностная мера аппроксимируется мерой доверия *bel* (нижняя мера) и мерой правдоподобия *pl* (верхняя мера), так что

$$0 \le bel(A) \le pl(A) \le 1.$$

Меры доверия и правдоподобия некоторым образом расщепляют вероятностную меру, что проявляется соотношениями

$$bel(A) + pl\left(\overline{A}\right) = 1, \; pl(A) + bel\left(\overline{A}\right) = 1.$$

Из этих соотношений вытекает, что

$$bel(A) + bel\left(\overline{A}\right) \le 1, \text{ а } pl(A) + pl\left(\overline{A}\right) \ge 1.$$

Мера доверия и мера правдоподобия, вообще говоря, неаддитивны. Они оказываются аддитивными, в случае совпадения (и в этом случае определяют вероятностную меру). Отсутствие аддитивности не позволяет определять математическое ожидание относительно мер доверия, используя интеграл Римана или Лебега. Это потребовало развить новые подходы к интегриро-

ванию относительно таких мер[5]. Широкое распространение, в частности, получил интеграл Шоке (см. [20]). Интегрирование по Шоке позволяет рассчитать математическое ожидание случайных величин относительно меры доверия и меры правдоподобия и получить интервальную оценку ожидаемого значения.

В работе описывается модель распространения доверия по графу атаки.

Граф атак служит для моделирования представления о том, как различные уязвимости могут сочетаться для атаки. Эксплойты существующих уязвимостей представляются в графовой модели переходами (дугами) соединяющими пред-условия с уязвимостями или уязвимости с пост-условиями.

Формально граф атак (см. [21, 22]) представляет собой направленный граф с множеством вершин $E \cup C$ и множеством дуг $R_r \cup R_i$, где

E — множество уязвимостей (эксплойтов),

C — множество условий,

$R_r \subseteq C \times E$, $R_i \subseteq E \times C$ — бинарные отношения.

Приведем типичный пример. Рассматривается простой сценарий, в котором файловый сервер (host 1) предлагает услуги передачи и приема данных по протоколам ftp, ssh и rsh; сервер баз данных (host 2) предлагает услуги передачи и приема данных по протоколам ftp и rsh. Межсетевой экран допускает только ftp, ssh и rsh-трафик с рабочей станции пользователя (host 0) на оба сервера. Множество E состоит из восьми эксплойтов:

ftp_rhosts(0,1), ftp_rhosts(0,2), ftp_rhosts(1,2),
rsh(0,1), rsh(0,2), rsh(1,2),
sshd_bof(0,1), local_bof(2,2)

(два индекса в скобках указывают соответственно на сервер отправки и сервер приема).

Множество C состоит из семи элементов:

trust(0,1), trust(0,2), trust(1,2), user(0), user(1), user(2), root(2).

Дуги описывают три возможных пути атаки:

sshd_bof(0,1) — ftp_rhosts(1,2) — rsh(1,2) — local_bof(2,2);

ftp_rhosts(0,1) — rsh(0,1) — ftp_rhosts(1,2) — rsh(1,2) — local_bof(2,2);

ftp_rhosts(0,2) — rsh(0,2) — local_bof(2,2).

Условия располагаются между эксплойтами, например, ftp_rhosts(1,2) — trust(1,2) — rsh(1,2),
и аналогично в других случаях.

Причинно-следственная связь между эксплойтами может быть конъюнктивной или дизъюнктивной в зависимости от того, как они связаны условиями. Более того, они могут быть взаимозависимы, что, естественно, может влиять на окончательную вероятность успеха атаки. Предполагается, что базовые вероятности приписываются уязвимостям на основе действующих стандартов информационной безопасности (например, CVSS) и экспертных оценок. Затем оценка вероятности атак проводится на основе баейесовских соотношений или комбинаторных расчетов, см. [13, 23-25]

Оценка вероятности атаки вычисляется по оценкам вероятности узлов на пути атаки. В свою очередь вероятность узла вычисляется по топологии графа. Родительские узлы могут быть логически связаны с анализируемым узлом дизъюнктивно, конъюнктивно, или более сложным образом. Это определяет способ расчета вероятности (доверия-правдоподобия). Метод оценки конъюнкций в рамках концепций Демпстера-Шефера был предложен в работах Шриваставы и соавторов[6], см. [18, 26, 27]. В настоящей работе описан подход, позволяющий производить оценку доверия-правдоподобия для произвольных булевых комбинаций свидетельств.

На экспертном уровне сценарии атаки могут быть увязаны с событиями, несущими угрозу информационной безопасности. Распределение вероятности в пространстве событий порождает распределение доверия в пространстве сценариев. Если потери, ассоциированные с реализацией сценариев, имеют количественную оценку, интегрирование по Шоке позволяет оценить математическое ожидание потерь относительно мер доверия и правдоподобия, и, тем самым, получить интервальную оценку ожидаемых потерь.

1. Оценка атаки на основе свидетельств

1.1. Меры доверия и правдоподобия на конечных фреймах

Основой для определения мер доверия и правдоподобия на конечном множестве (фрейме) Θ служит базовое распределение вероятностей, т.е. такая функция множеств $m: 2^{\Theta} \to [0,1]$, что $\sum_{X \subseteq \Theta} m(X) = 1$.

Множества $X \subseteq \Theta$, для которых $m(X) \neq 0$, называются фокальными. Базовое распределение вероятностей имеет следующую интерпретацию. Элементы фрейма соответствуют потенциально возможным ответам на поставленный вопрос. Величина $m(X)$ ука-

5 Denneberg D. Non-additive Measure and Integral. Dordrecht: Kluwer, 1994. 178 p.

6 Srivastava R. P., Mock T. J., Turner J. L. Analytical formulas for risk assessment for a class of problems where risk depends on three interrelated variables // International Journal of Approximate Reasoning. 2007. № 1 (45). p. 123-151.

зывает вероятность того, что верный ответ находится в множестве X. Величина $m(\varnothing)$ — это вероятность того, что в множестве Θ отсутствует верный ответ. Если $m(\varnothing)=0$, базовое распределение вероятностей называется нормализованным, если $m(\varnothing)=1$ — противоречивым. Произвольное непротиворечивое базовое распределение вероятностей m несложно нормализовать, полагая

$$m^*(X)=\frac{m(X)}{1-m(\varnothing)}$$

при $X\neq\varnothing$ и $m^*(\varnothing)=0$.

Рассмотрим бинарный фрейм $\Theta=\{a^+,a^-\}$, состоящий из двух элементов, содержательно соответствующих ответам «да» и «нет». Базовое распределение вероятности на бинарном фрейме (не обязательно нормализованное) может быть задано четверкой чисел

$\mu=m(a^+)$; $\nu=m(a^-)$; $\pi=m(a^+,a^-)$; $\lambda=m(\varnothing)$,

таких, что

$$\mu+\nu+\pi+\lambda=1,\ \mu,\nu,\pi,\lambda\geq 0.$$

Если распределение доверия нормализовано, то применительно, например, к уязвимости первое число может быть интерпретировано как субъективная оценка доводов в пользу того, что уязвимость будет использована в атаке, второе — как субъективная оценка доводов в пользу того, что уязвимость не будет использована. Величина $\pi=1-\mu-\nu$ служит оценкой неопределенности.

Базовое распределение порождает на конечном фрейме Θ меру доверия *bel* и меру правдоподобия *pl*:

$$bel(X)=\sum_{Y\subseteq X,Y\neq\varnothing}m(Y),\ pl(X)=\sum_{Y\cap X\neq\varnothing}m(Y). \quad (1)$$

Легко видеть, что

$$bel(X)+pl(\bar{X})=1, \quad (2)$$

где $\bar{X}=\Theta\setminus X$ — дополнение множества X относительно фрейма Θ.

Зная меру доверия, можно восстановить функцию базового распределения вероятности:

$$m(X)=\sum_{Y\subseteq X}(-1)^{|X|-|Y|}(1+bel(Y)-bel(\Theta)),$$

где $|X|$ обозначает число элементов конечного множества X. Аналогичным образом функция базового распределения вероятности восстанавливается по мере правдоподобия.

Комбинирование мер доверия

Для описания динамики переноса доверия используется правило комбинирования свидетельств Демпстера.

Пусть имеется некоторый конечный фрейм Θ. Информация об элементах фрейма представлена свидетельством, формальным выражением которого служит базисное распределение вероятности m_1. Предположим, появилось второе свидетельство, и ему соответствует базисное распределение вероятности m_2. Правило Демпстера позволяет построить комбинированное нормализованное базисное распределение вероятности $m_1\oplus m_2$, если m_1 и m_2 совместимы, т.е. $\sum_{X\cap Y=\varnothing}m_1(X)m_2(Y)\neq 1$. А именно, если $Z\neq\varnothing$, то

$$(m_1\oplus m_2)(Z)=k\sum_{X\cap Y=Z}m_1(X)m_2(Y), \quad (3)$$

где

$$k=(1-\sum_{X\cap Y=\varnothing}m_1(X)m_2(Y))^{-1} - \quad (4)$$

нормализующий множитель.

Рассмотрим комбинирование базисных распределений на бинарном фрейме $\Theta=\{a^+,a^-\}$. Пусть $\mu_i=m_i(a^+)$, $\nu_i=m_i(a^-)$, где m_i, $i=1,2$, — совместимые нормализованные распределения. Тогда для $\mu=(m_1\oplus m_2)(a^+)$, $\nu=(m_1\oplus m_2)(a^-)$ имеем

$$\mu=1-\frac{(1-\mu_1)(1-\mu_2)}{1-(\mu_1\nu_2+\mu_2\nu_1)};$$
$$\nu=1-\frac{(1-\nu_1)(1-\nu_2)}{1-(\mu_1\nu_2+\mu_2\nu_1)}. \quad (5)$$

В дальнейшем будет использоваться еще один вариант комбинирования функций распределения доверия:

$$(m_1\odot m_2)(Z)=\sum_{X\cap Y=Z}m_1(X)m_2(Y), \quad (6)$$

отличающийся от комбинирования по Демпстеру отсутствием нормировочного множителя. Такую операцию будем называть ненормализованной комбинацией свидетельств (или функций распределения вероятности).

1.2. Распространение доверия по графу атак

Для оценки уязвимости информационной сети в целом можно строить граф атаки из отдельных базовых блоков (см. [28]). Каждый из блоков описывает логическую связь узлов-родителей с их прямым потомком. Простейший вариант связи — последовательное соединение узлов: уязвимость *A* создает условие для использования уязвимости *B*, а последовательное использование уязвимостей *A* и *B* позволяет злоумышленнику добиться целевого состояния. Более сложные связи описываются через конъюнкции и дизъюнкции.

Например, использование одной из уязвимостей *A* или *B* позволяет воспользоваться уязвимостью *C*, и т.п. Более того, между родительскими узлами возможно наличие зависимости, приводящее к корректировке оценки логических формул.

При баейсовском подходе каждый узел получает вероятностную оценку вида (μ,ν), где $\mu,\nu \geq 0$ и $\mu+\nu=1$. Механизм байесовских вычислений обеспечивает перенос вероятности по графу (см. [29]). Применение оценок с использование мер доверия и комбинирование свидетельств позволяют получить модель переноса доверия в условиях большей неопределенности, когда, вообще говоря, $\mu+\nu \leq 1$.

В этом разделе мы опишем механизм переноса доверия, используя в качестве отправной точки идеи из [30].

Пусть A_i, $i=1,2,...,n$, — родительские узлы для узла B на графе атаки и $U(X_1,...,X_n)$ — дизъюнктивная нормальная форма, определяющая логическую связь узлов A_i с узлом B. Основанием для оценки узла A_i служит свидетельство с базисной функцией распределения доверия m_i на бинарном фрейме $\Theta_i=\{a_i^+,a_i^-\}$. Оценка узла A_i задается парой чисел (μ_i,ν_i), где $\mu_i=m_i(a_i^+)$, $\nu_i=m_i(a_i^-)$. Соответственно, $m_i(\Theta_i)=\pi_i$ и $\mu_i+\nu_i+\pi_i=1$.

Аналогичным образом имеется свидетельство с базовой функцией распределения m_B на бинарном фрейме $\Theta_B=\{a_B^+,a_B^-\}$, дающее оценку возможности атаки через узел B.

Оценка возможности атаки через узлы A_i и B строится следующим образом. Сначала в терминах доверия-правдоподобия оценивается формула $U(X_1,...,X_n)$. Эта оценка дает базовое распределение вероятности на бинарном фрейме $\Theta_B=\{a_B^+,a_B^-\}$ такое, что $m_U(a_B^+)=bel(U)$, $m_U(a_B^-)=1-pl(U)$. Итоговая оценка атаки получается комбинированием свидетельств m_U и m_B, и имеет базовое распределение $m_U \oplus m_B$.

Приведем описание того, как строится оценка формулы $U(X_1,...,X_n)$.

Вообще, говоря, свидетельства E_i могут быть взаимосвязаны. Интенсивность связи мы будем оценивать числом из промежутка $[0,1]$. А именно, пусть $I \subseteq \{1,2,...,n\}$ некоторое множество индексов. Зависимость между свидетельствами с номерами из множества индексов I будем представлять числом $p_I \in [0,1]$ (заметим, что в работах Шриваставы и соавторов (см. сноску в п. 1.1) интенсивность связи использовалась лишь в двучленных конъюнкциях).

Составим вспомогательный фрейм Θ'. Его элементами служат некоторые слова вида

$$w=z^{\omega}a_1^{\omega_1}a_2^{\omega_2}...a_n^{\omega_n}, \quad (7)$$

где $\omega,\omega_1,...,\omega_n \in \{+,-\}$. Для слова w вида (7) определим бинарный вектор $x=\varphi(w) \in \{0,1\}^n$ следующим образом:

если $\omega_i=+$, то $x_i=1$; если $\omega_i=-$, то $x_i=0$.

Слово w вида (7) является элементом фрейма Θ', если для вектора $x=\varphi(w)$ выполняется одно из следующих условий:

1) $U(x_1,...,x_n)=1$ и $\omega=+$;
2) $U(x_1,...,x_n)=0$ и $\omega=-$.

Для каждого $i=1,2,...,n$ обозначим через m_i' цилиндрическое продолжение базисного распределения m_i с Θ_i на Θ':

$$m_i'(\{w=z^{\omega}a_1^{\omega_1}a_2^{\omega_2}...a_n^{\omega_n} \in \Theta' \mid \omega_i=+\})=\mu_i;$$
$$m_i'(\{w=z^{\omega}a_1^{\omega_1}a_2^{\omega_2}...a_n^{\omega_n} \in \Theta' \mid \omega_i=-\})=\nu_i;$$
$$m_i'(\Theta')=\pi_i.$$

Чтобы учесть связь между свидетельствами $E_i, i \in I$, выделим во фрейме Θ' подмножество W_I, которое содержит все слова $w \in \Theta'$ с $\omega=+$, а также те слова $w \in \Theta'$ с $\omega=-$, которые обладают следующим свойством: если поменять в векторе $x=\varphi(w)$ все значения x_i на противоположные значения $1-x_i$, значение, принимаемое формулой U, изменится с 0 на 1. Зададим на фрейме Θ' базисное распределение доверия m_I', полагая

$$m_I'(W_I)=p_I;\ m_I'(\Theta')=1-p_I.$$

Положим

$$m'=m_I' \odot m_1' \odot ... \odot m_n'.$$

Пусть θ — проекция фрейма Θ' на бинарный фрейм $\Theta=\{z^+,z^-\}$, при которой $\theta(w)=z^{\omega}$, если $w=z^{\omega}a_1^{\omega_1}a_2^{\omega_2}...a_n^{\omega_n} \in \Theta'$. Обозначим через m_θ' базисное распределение доверия на фрейме $\Theta_B=\{a_B^+,a_B^-\}$ такое, что

$$m_\theta'(a_B^{\omega})=\sum_{\theta(X)=z^{\omega}} m'(X);\ m_\theta'(\Theta_B)=m'(\Theta').$$

Распределение m_θ' может оказаться ненормализованным. Его нормализация и дает логическую оценку формулы U в терминах доверия-правдоподобия:

$$bel(U)=\frac{m_\theta'(z^+)}{m_\theta'(z^+)+m_\theta'(z^-)+m_\theta'(\Theta)};$$
$$pl(U)=1-\frac{m_\theta'(z^-)}{m_\theta'(z^+)+m_\theta'(z^-)+m_\theta'(\Theta)}.$$

1.3. Пример оценки атаки

Рассмотрим ситуацию, когда уязвимость узла B, может быть использована для атаки при условии, что атакующему удалось использовать уязвимости узлов

A_1 и A_2. В этом случае $U = X_1 \wedge X_2$. Фрейм Θ' содержит четыре слова:

$$\Theta' = \{z^+a_1^+a_2^+, z^-a_1^+a_2^-, z^-a_1^-a_2^+, z^-a_1^-a_2^-\}.$$

Предположим, что связь узлов A_1 и A_2 выражает утверждение типа: если удалось воспользоваться одной из уязвимостей, то, вероятно, удастся воспользоваться и другой. Пусть число $q \in [0,1]$ указывает силу этой связи. Формально для представления этой связи выделим в Θ' подмножество

$$\Theta_{12} = \{z^+a_1^+a_2^+, z^-a_1^-a_2^-\}$$

и зададим распределение доверия на фрейме Θ', полагая

$$m'_{12}(\{z^+a_1^+a_2^+, z^-a_1^-a_2^-\}) = q;\ m'_{12}(\Theta') = p,$$

где $p = 1 - q$.

Значение $q = 0$ означает отсутствие связи (независимость свидетельских оценок доверия-правдоподобия для рассматриваемых уязвимостей), значение $q = 1$ – наличие максимально возможной связи (если использована одна уязвимость, будет использована и другая).

Цилиндрические продолжения функций распределения доверия m_1 и m_2 задаются следующими формулами:

$$m'_1(\{z^+a_1^+a_2^+, z^-a_1^+a_2^-\}) = \mu_1;$$
$$m'_1(\{z^-a_1^-a_2^+, z^-a_1^-a_2^-\}) = \nu_1;\ m'_1(\Theta') = \pi_1;$$
$$m'_2(\{z^+a_1^+a_2^+, z^-a_1^-a_2^+\}) = \mu_2;$$
$$m'_2(\{z^-a_1^+a_2^-, z^-a_1^-a_2^-\}) = \nu_2;\ m'_2(\Theta') = \pi_2.$$

Теперь вычисляем $m' = m'_{12} \odot m'_1 \odot m'_2$. Имеем (см. (6)):

$$m'(Z) = \sum_{W \cap X \cap Y = Z} m_{12}(W) m_1(X) m_2(Y).$$

Таким образом, получаем:

$$m'(\Theta') = p\pi_1\pi_2;$$
$$m'(\{z^+a_1^+a_2^+, z^-a_1^+a_2^-\}) = p\mu_1\pi_2;$$
$$m'(\{z^-a_1^-a_2^+, z^-a_1^-a_2^-\}) = p\nu_1\pi_2;$$
$$m'(\{z^+a_1^+a_2^+, z^-a_1^-a_2^+\}) = p\pi_1\mu_2;$$
$$m'(\{z^-a_1^+a_2^-, z^-a_1^-a_2^-\}) = p\pi_1\nu_2;$$
$$m'(\{z^+a_1^+a_2^+, z^-a_1^-a_2^-\}) = q\pi_1\pi_2;$$
$$m'(\{z^+a_1^+a_2^+\}) = q\mu_1\mu_2 + p\mu_1\mu_2 + q\pi_1\mu_2 + q\mu_1\pi_2;$$
$$m'(\{z^-a_1^+a_2^-\}) = p\mu_1\nu_2;$$
$$m'(\{z^-a_1^-a_2^+\}) = p\nu_1\mu_2;$$
$$m'(\{z^-a_1^-a_2^-\}) = q\nu_1\pi_2 + q\pi_1\nu_2 + p\nu_1\nu_2 + q\nu_1\nu_2;$$
$$m'(\varnothing) = q\mu_1\nu_2 + q\nu_1\mu_2.$$

Теперь находим маргинальное распределение доверия m'_θ на фрейме $\Theta_B = \{a_B^+, a_B^-\}$. Так как $\theta(X) = z^+$ при $X = \{z^+a_1^+a_2^+\}$, то

$$m'_\theta(a_B^+) = m'(\{z^+a_1^+a_2^+\}) = q\mu_1\mu_2 + p\mu_1\mu_2 + q\pi_1\mu_2 + q\mu_1\pi_2 = \mu_1\mu_2 + q(\pi_1\mu_2 + \mu_1\pi_2).$$

Далее, $\theta(X) = z^-$ при $X = \{z^-a_1^-a_2^+, z^-a_1^-a_2^-\}$; $X = \{z^-a_1^+a_2^-, z^-a_1^-a_2^-\}$; $X = \{z^-a_1^+a_2^-\}$; $X = \{z^-a_1^-a_2^+\}$; $X = \{z^-a_1^-a_2^-\}$.

Значит,

$$m'_\theta(a_B^-) = p\nu_1\pi_2 + p\pi_1\nu_2 + p\mu_1\nu_2 + p\nu_1\mu_2 + \nu_1\pi_2 + \pi_1\nu_2 + p\mu_1\nu_2 + p\nu_1\mu_2 + \nu_1\nu_2 + p\nu_1\mu_2 + q\nu_1\pi_2 + q\pi_1\nu_2 + p\nu_1\nu_2 + q\nu_1\nu_2 =.$$

Наконец, $\theta(X) = \Theta$ при $X = \{z^+a_1^+a_2^+, z^-a_1^+a_2^-\}$; $X = \{z^+a_1^+a_2^+, z^-a_1^-a_2^+\}$; $X = \{z^+a_1^+a_2^+, z^-a_1^-a_2^-\}$; $X = \Theta'$, а $\theta(X) = \varnothing$ при $X = \varnothing$. Следовательно,

$$m'_\theta(\varnothing) = q(\mu_1\nu_2 + \nu_1\mu_2);$$
$$m'_\theta(\Theta) = p\pi_1\pi_2 + q\pi_1\pi_2 + p\mu_1\pi_2 + p\pi_1\mu_2 = \pi_1\pi_2 + p(\mu_1\pi_2 + \pi_1\mu).$$

Положим

$$G = \mu_1\pi_2 + \pi_1\mu_2;\ H = \mu_1\nu_2 + \nu_1\mu_2.$$

Обозначим через $m*$ нормализованную функцию распределения доверия, ассоциированную с m'_θ. Тогда нормализующий множитель можно представить как $(1 - qH)^{-1}$ (см. (4)), и, значит,

$$m*(a_B^+) = \frac{\mu_1\mu_2 + qG;}{1 - qH}$$

$$m*(a_B^-) = 1 - \frac{(1-\nu_1)(1-\nu_2)}{1-qH} \quad (8)$$

в соответствии с (5).

Формулы (8) и дают логическую оценку формулы U:

$$bel(U) = \frac{\mu_1\mu_2 + qG}{1-qH};\ pl(U) = \frac{(1-\nu_1)(1-\nu_2)}{1-qH}.$$

Оценка атаки через блок узлов A_1, A_2, B получается комбинированием функций распределения доверия $m*$ и m_B. Таким образом, возможность атаки $(A_1 \wedge A_2) \to B$ оценивается следующим образом:

$$bel((A_1 \wedge A_2) \to B) = \frac{\mu^* \mu_B}{1-(\mu^* \nu_B + \nu^* \mu_B)};$$

$$pl((A_1 \wedge A_2) \to B) = \frac{(1-\nu^*)(1-\nu_B)}{1-(\mu^* \nu_B + \nu^* \mu_B)},$$

где $\mu^* = bel(U)$, $\nu^* = 1 - pl(U)$, а μ_B и ν_B – оценки для узла B.

В заключение рассмотрим числовой пример. Предположим для определенности, что вероятность использования уязвимостей в узлах A_1, A_2, B получила интервальные оценки:

$$0{,}1 \le \Pr(A_1) \le 0{,}15;\ 0{,}2 \le \Pr(A_2) \le 0{,}3;$$
$$0{,}15 \le \Pr(B) \le 0{,}25.$$

Тогда в терминах функций доверия можно считать что

$$\mu_1 = 0{,}1;\ \nu_1 = 0{,}85;\ \mu_2 = 0{,}2;$$
$$\nu_2 = 0{,}7;\ \mu_B = 0{,}15;\ \nu_B = 0{,}75.$$

Тогда

$$\pi_1 = 0{,}05;\ \pi_2 = 0{,}15.$$

Далее,

$$G = 0{,}1 \cdot 0{,}15 + 0{,}05 \cdot 0{,}2 = 0{,}025;$$
$$H = 0{,}1 \cdot 0{,}7 + 0{,}85 \cdot 0{,}2 = 0{,}24.$$

Пусть $q = 0{,}5$. Найдем оценку конъюнкции $U = A_1 \wedge A_2$ в терминах доверия:

$$bel(U) = \frac{0{,}1 \cdot 0{,}2 + 0{,}5 \cdot 0{,}025}{1 - 0{,}5 \cdot 0{,}24} = 0{,}037;$$

$$pl(U) = \frac{0{,}15 \cdot 0{,}3}{1 - 0{,}5 \cdot 0{,}24} = 0{,}051.$$

Таким образом, можно считать, что с учетом зависимости узлов A_1 и A_2 вероятность атаки через конъюнкцию $A_1 \wedge A_2$ лежит в промежутке от 0,037 до 0,051. Теперь мы можем найти оценки в терминах доверия для атаки A:

$$bel(\mathrm{A}) = \frac{0{,}037 \cdot 0{,}15}{1 - (0{,}037 \cdot 0{,}75 + 0{,}949 \cdot 0{,}15)} = 0{,}0067;$$

$$pl(\mathrm{A}) = \frac{0{,}051 \cdot 0{,}25}{1 - (0{,}037 \cdot 0{,}75 + 0{,}949 \cdot 0{,}15)} = 0{,}0153.$$

Если вместо интервальных оценок для уязвимостей A_1, A_2 и B использовать средние значения и не учитывать зависимость между A_1 и A_2, вероятность атаки A составляет 0,0063.

2. Интегрирование по Шоке и оценка последствий реализации рисков атаки

2.1. Интеграл Шоке

Понятие интеграла Шоке было введено в 1953 г., но применения начались после теоретического осмысления лишь в конце восьмидесятых годов. За прошедшие годы интеграл Шоке был использован для решения самых разных прикладных задач, см. [17, 19 31].

В этом разделе мы приведем основные сведения об интеграле Шоке, необходимые для вычисления математического ожидания относительно функций доверия и правдоподобия.

Пусть Ω – множество и $\boldsymbol{A} \subseteq 2^{\Omega}$ – алгебра его подмножеств. Далее, пусть $\mu : \boldsymbol{A} \to [0, +\infty)$ монотонная функция множеств, такая, что $\mu(\varnothing) = 0$ (монотонность означает, что $X \subseteq Y$ влечет $\mu(X) \le \mu(Y)$). Техника интегрирования по Шоке позволяет рассматривать μ как меру и интегрировать относительно нее вещественнозначные функции.

Пусть $f(\omega)$ – функция на Ω, принимающая неотрицательные значения. Определим соответствующую ей функцию распределения $F(x)$ на множестве действительных чисел, полагая

$$F(x) = \mu(f(\omega) > x),$$

где, как обычно, $f(\omega) > x$ – сокращенное обозначение для $\{\omega \in \Omega \mid f(\omega) > x\}$.

Если функция μ определена на всех подмножествах множества Ω, т.е. $\boldsymbol{A} = 2^{\Omega}$, интеграл Шоке определяется равенством

$$\int_{\Omega} f d\mu = \int_0^{\infty} F(x) dx,$$

где в левой части интеграл Шоке, а в правой – интеграл Римана.

Если $\boldsymbol{A}$ – собственное подмножество множества 2^{Ω}, сначала определяются числовые функции μ^* и μ_* так, что

$$\mu^*(X) = \inf\{\mu(Y) \mid X \subseteq Y, Y \in \boldsymbol{A}\},$$
$$\mu_*(X) = \sup\{\mu(Y) \mid Y \subseteq X, Y \in \boldsymbol{A}\}.$$

Функция $f(\omega)$ считается интегрируемой если,

$$-\infty < \int_{\Omega} f d\mu^* = \int_{\Omega} f d\mu_* < \infty$$

а общее значение берется в качестве значения интеграла Шоке $\int_{\Omega} f d\mu$.

При интегрировании относительно мер доверия и правдоподобия множество Ω оказывается конечным и, кроме того, $\mu(\Omega) = 1$. С учетом этого, вычисление интеграла Шоке может быть выполнено следующим образом.

Упорядочим значения функции $f(\omega)$ по убыванию так, что

$$f(\Omega) = \{s_1, \ldots, s_m\} \text{ и } s_1 > s_2 > \ldots > s_m.$$

Пространство Ω разбивается на попарно непересекающиеся множества

$$A_i = \{\omega \mid f(\omega) = s_i\}\ ,\ i = 1,2,...,m\ .$$

Положим

$$\Delta\mu_i = \mu\ (A_1 \cup ... \cup A_i) - \mu(A_1 \cup ... \cup A_{i-1})\ ,$$
$$i = 1,2,...,m\ .$$

Заметим, что $\Delta\mu_1 = \mu\ (A_1) - \mu(\varnothing) = \mu(A_1)$.

Тогда

$$\int_\Omega f d\mu = s_1\Delta\mu_1 + s_2\Delta\mu_2 + ... + s_m\Delta\mu_m\ . \quad (9)$$

Несложно проверить, что справедливо также равенство

$$\int_\Omega f d\mu = \sum_{i=1}^{m} (s_i - s_{i+1})\mu(A_1 \cup ... \cup A_i)\ . (10)$$

Замечание. Интеграл Шоке, вообще говоря, не обладает свойством аддитивности. В общем случае интеграл $\int_\Omega (f+g)d\mu$ может не равняться сумме интегралов $\int_\Omega f d\mu$ и $\int_\Omega g d\mu$. Равенство можно гарантировать для так называемых комонотонных функций, т.е. таких функций f и g что невозможно одновременное выполнение неравенств $f(\omega_1) < f(\omega_2)$ и $g(\omega_1) > g(\omega_2)$, каковы бы ни были $\omega_1, \omega_2 \in \Omega$.

2.2. Мера доверия в пространстве сценариев и оценка ожидаемого ущерба

Рассмотрим ситуацию, когда для каждого семейства сценариев атак X указаны верхняя и нижняя оценка возможности реализации хотя бы одного сценария из этого семейства. Будем обозначать их соответственно $pl(X)$ и $bel(X)$. Напомним содержательную интерпретацию верхней оценки: $1 - pl(V)$ — оценка вероятности того, что ни один сценарий из семейства X не реализуется. Такое распределение можно получить с помощью переноса доверия методами, описанными в разделе 3.2. Для этого можно, например, составить из уязвимостей объединенный граф всех атак, соответствующих сценариям из X, и применить технику распространения доверия по минимальному остовному дереву (см. обзор современных методов в [29, 32, 33]).

В этом параграфе мы опишем подход, который основывается на статистических оценках событий и событийного описания сценариев атак. Предлагаемая формализация основывается на комбинации идей Демпстера-Шефера и интегрирования по Шоке.

Пусть A — множество всевозможных сценариев атак, а E — множество событий. Под событиями понимаются стандартизованные события, угрожающие информационной безопасности. Например, пространство событий E может быть сформировано на основе списка событий, представленного в руководстве «Information Security. Guide for Conducting Risk Assessments. NIST Special Publication 800-30, Appendix E. Threat Events»[7], в котором содержится описание более, чем 120 типовых событий. События должны быть типовыми для того, чтобы имелась достаточная статистическая база для оценки их вероятности. В множество E включается также «пустое» событие «ничего не произошло». Будем предполагать, что в пространстве событий задано распределение вероятностей (в обычном смысле). Для события $e \in E$ обозначим через $\Pr(e)$ его вероятность. С учетом пустого события выполняется соотношение $\sum_{e \in E} \Pr(e) = 1$.

Базовой структурой для определения функции емкости (в смысле Шоке) в пространстве сценариев служит отношение совместимости $G \subseteq E \times A$, связывающее события и сценарии. Отношение G представляется бинарной матрицей, строки которой соответствуют событиям, столбцы – сценариям. Если $X \subseteq A$ семейство сценариев, определяем емкость $m(X)$, полагая

$$m(X) = \sum \{\Pr(e) | G(e) = X\}\ ,$$

где, через $G(e)$ обозначено множество всех сценариев, связанных с событием e .

Семейства сценариев, емкость которых отлична от нуля, называются фокальными.

Используя емкости, можно определить меры доверия и правдоподобия (см. (1), (2)):

$$bel(X) = \sum \{m(Y) | Y \subseteq X\}; \quad (11)$$
$$pl(X) = \sum \{m(Y) | Y \cap X \neq \varnothing\}. \quad (12)$$

Очевидно, эти меры монотонны и, кроме того, $bel(X) \le pl(X)$.

Для семейства сценариев X обозначим через $\bar{X}$ дополнение семейства X (относительно A). Поскольку условия $Y \subseteq X$ и $Y \cap \bar{X} = \varnothing$ равносильны, и $\sum_{Y \subseteq S} m(Y) = 1$, получаем соотношение

$$bel(X) + pl(\bar{X}) = 1,$$

справедливое для любого семейства сценариев X .

Предположим, что для каждого сценария a определен количественный показатель ущерба от его реализации $S(a)$. Математическое ожидание величины S относительно меры доверия и меры правдоподобия дают соответственно верхнюю и нижнюю оценку ожидаемого ущерба.

7 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (последнее обращение 22.01.2023)

Таблица 1

Вероятности событий

Событие	e_1	e_2	e_3	e_4	e_5	e_6	e_7
Вероятность	0.1	0.05	0.1	0.2	0.2	0.3	0.05

Таблица 2

Сценарии и события

Сценарий	e_1	e_2	e_3	e_4	e_5	e_6	e_7	Ущерб
a_1	1	0	0	0	0	0	0	5
a_2	0	1	1	0	0	0	0	8
a_3	0	3	0	0	1	0	0	8
a_4	0	0	0	1	0	1	0	2
a_5	0	1	1	1	0	1	0	10
a_6	0	0	0	0	0	0	1	0

Пример. Пусть пространство E состоит из следующих событий:

e_1 — создание дубликатов веб-сайтов;

e_2 — установка вредоносного ПО;

e_3 — компрометация логической защиты корпоративных брандмауэров;

e_4 — получение доступа к каналам передачи информации;

e_5 — получение несанкционированного доступа;

e_6 — неправильное обращение с конфиденциальной информацией авторизованных пользователей;

e_7 — ничего из перечисленного выше.

Вероятности событий представлены в табл. 1

В таблице 2 задано отношение совместимости событий и сценариев. Кроме того в последнем столбце таблицы 2 для каждого сценария приведена оценка ущерба (severity) от его реализации. Оценка произведена по получисленной шкале 1-10 (10 – очень высокий, 8 – высокий, 5 – умеренный, 2 – незначительный, 0 – пренебрежимо малый).

В соответствии с таблицей 2 в пространстве сценариев имеется шесть фокальных множеств со следующими значениями емкости:

$$m(\{a_1\}) = P(e_1) = 0.1;\ m(\{a_2, a_3, a_5\}) = P(e_2) = 0.05;$$

$$m(\{a_2, a_5\}) = P(e_3) = 0.1;$$

$$m(\{a_4, a_5\}) = P(e_4) + P(e_6) = 0.5;$$

$$m(\{a_3\}) = P(e_5) = 0.2;\ m(\{a_6\}) = P(e_6) = 0.05.$$

Далее,

$A_1 = S^{-1}(10) = \{a_5\};\ A_2 = S^{-1}(8) = \{a_2, a_3\}$,

$A_3 = S^{-1}(5) = \{a_1\}$,

$A_4 = S^{-1}(2) = \{a_4\},\ A_5 = S^{-1}(0) = \{a_6\}$.

Для всех $j = 1,\ldots,5$, используя (11) и (12), находим

$$b_j = bel\left(\bigcup_{i=1}^{j} A_i\right) \text{ и } p_j = pl\left(\bigcup_{i=1}^{j} A_i\right)$$

(см. таб. 3).

Таблица 3

Математическое ожидание по Шоке

j	1	2	3	4	5
s_j	10	8	5	2	0
$s_j - s_{j+1}$	2	3	3	2	0
b_j	0	0.35	0.45	0.95	1.0
p_j	0.65	0.85	0.95	1	1.0

По формуле (10) получаем

$E_{bel}(S) = 2 \cdot 0 + 3 \cdot 0.35 + 3 \cdot 0.45 + 2 \cdot 0.95 + 0 \cdot 1.0 = 4.3$;

$E_{pl}(S) = 2 \cdot 0.65 + 3 \cdot 0.85 + 3 \cdot 0.95 + 2 \cdot 0.1 + 0 \cdot 1.0 = 8.7$.

Таким образом, можно считать, что оценка ожидаемого ущерба находится в промежутке от 4.3 до 8.7, т.е. примерно от умеренного до высокого. Для получения точечной оценки можно воспользоваться кри-

терием Гурвица с постоянной оптимизма-пессимизма γ и представить интегральный критерий в виде

$$E_\gamma(S) = (1-\gamma)E_{bel}(S) + \gamma E_{pl}(S).$$

Тогда в рассматриваемом примере $E_\gamma(S) = 8.7 - 3.6\gamma$. Высокий уровень ущерба ожидается при значении постоянной оптимизма $\gamma = 0.2$.

Заключение

Предложен метод распространения доверия по графу атак. Особенность метода в оригинальном подходе к истинностной оценке булевых комбинаций свидетельств. Предполагается, что в качестве исходной информации для каждого узла указывается интервальная оценка вероятности того, что атака через данный узел окажется успешной. Эта информация трансформируется в свидетельства на бинарных фреймах, что позволяет использовать технику теории свидетельств. Свидетельства на бинарных фреймах допускают прозрачную логическую интерпретацию, давая, по существу, оценку истинности утверждений в терминах неклассической многозначной логики. Оценка истинности булевых комбинаций свидетельств как раз и выполняется в рамках этой логики. Обратная интерпретация логических оценок позволяет трактовать их как меры доверия и правдоподобия.

Недостатком метода является необходимость проведения алгебраических вычислений, объем которых быстро растет с ростом сложности логических формул.

Кроме этого, предложен подход к оценке ожидаемого ущерба, в случае, когда в пространстве сценариев атак заданы распределения доверия и правдоподобия. Метод основывается на вычислении математического ожидания ущерба по мерам доверия и правдоподобия с использованием интеграла Шоке. Предложен подход к заданию мер доверия и правдоподобия в пространстве сценариев на основе вероятностной оценки типовых событий информационной безопасности. Несмотря на простоту, подход позволяет получить вполне реалистичные оценки, которые могут служить основой для более точного анализа.

Косвенным доводом в пользу предлагаемого использования мер доверия и правдоподобия может служить то, что близкие подходы хорошо зарекомендовали себя в финансовом аудите.

Литература

1. Попов Е., Семячков К. Умные города. Монография. – М.: Юрайт, 2020. 347 С.
2. Innovations in Cybersecurity Education. Kevin Daimi, Guillermo Francia, eds. Springer 2020. 391 P. https://doi.org/10.1007/978-3-030-50244-7
3. Мамаева Л. Н., Бехер В. В. Угрозы кибербезопасности в цифровом пространстве //Вестник Саратовского государственного социально-экономического университета. 2019. № 4 (78). С. 68-70.
4. Гаськова Д. А., Массель А. Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2 (30). С. 42-49.
5. Review of cybersecurity risk analysis methods and tools for safety critical industrial control systems. VTT Technical Research Centre of Finland. VTT Research Report. VTT-R-00298-22. 2022. 46 p. https://cris.vtt.fi/en/publications/review-of-cybersecurity-risk-analysis-methods-and-tools-for-safet (последнее обращение 22.01.2023)
6. Upadhyay D., Sampalli S. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations // Computers & Security. – 2020. V. 89. P. 101666.
7. Калашников А. О., Бугайский К. А. Модель оценки безопасности сложной сети (часть 1) // Вопросы кибербезопасности. 2022. №. 4 (50). С. 26-38. DOI:10.21681/2311-3456-2022-4-26-38
8. Landoll D. The security risk assessment handbook: A complete guide for performing security risk assessments. Boca Raton: CRC Press, 2021. 512 P. https://doi.org/10.1201/9781003090441
9. Petturiti D., Vantaggi B. How to assess coherent beliefs: a comparison of different notions of coherence in Dempster-Shafer theory of evidence // In Reflections on the Foundations of Probability and Statistics: Essays in Honor of Teddy Seidenfeld. Cham : Springer International Publishing, 2022. С. 161-185.
10. Лепский А. Е. Анализ противоречивости информации в теории функций доверия. Ч. 1. Внешний конфликт // Проблемы управления. 2021. №. 5. С. 3-19.
11. Иванов В. К., Виноградова, Н. В., Палюх, Б. В., & Сотников, А. Н. Современные направления развития и области приложения теории Демпстера-Шафера (обзор) // Искусственный интеллект и принятие решений. 2018. №. 4. С. 32-42.
12. Naik N., Jenkins P., Kerby B., Sloane J., Yang L. Fuzzy logic aided intelligent threat detection in cisco adaptive security appliance 5500 series firewalls. In 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). – IEEE, 2018. P. 1-8.
13. Гузаиров М. Б. Вульфин А. М., Картак В. М., Кириллова, А. Д., Миронов К. В. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности // Труды Института системного анализа Российской академии наук. 2019. № 4 (69). С. 62-69. DOI: 10.14357/20790279190408
14. Калашников А. О., Бугайский К. А. Модель оценки безопасности сложной сети (часть 2) // Вопросы кибербезопасности. 2022. № 5 (50). С. 47-60. DOI:10.21681/2311-3456-2022-5-47-60
15. Канеман Д., Сибони О., Санстейн К.Р. Шум. М.: АСТ, 2021. 590 С.

16. Bruine de Bruin W., Carman K. G. Measuring subjective probabilities: The effect of response mode on the use of focal responses, validity, and respondents' evaluations //Risk Analysis. 2018. № 10 (38). С. 2128-2143. DOI: 10.1111/risa.13138
17. Wilson R. S., Zwickle A., Walpole H. Developing a broadly applicable measure of risk perception //Risk Analysis. 2019. № 4 (39). С. 777-791.
18. Zhang, Z., Jiang, C. Evidence-theory-based structural reliability analysis with epistemic uncertainty: a review. Struct Multidisc Optim 63, 2935–2953 (2021). https://doi.org/10.1007/s00158-021-02863-w
19. Jiroušek R., Kratochvíl V. On subjective expected value under ambiguity // International Journal of Approximate Reasoning. 2020. Т. 127. С. 70-82. https://doi.org/10.1016/j.ijar.2020.09.002
20. Dimuro G. P. Fernández, J., Bedregal, B., Mesiar, R., Sanz, J. A., Lucca, G., Bustince, H. The state-of-art of the generalizations of the Choquet integral: from aggregation and pre-aggregation to ordered directionally monotone functions // Information Fusion. 2020. V. 57. P. 27-43. https://doi.org/10.1016/j.inffus.2019.10.005
21. Lallie H. S., Debattista K., Bal J. A review of attack graph and attack tree visual syntax in cyber security //Computer Science Review. 2020. Т. 35. С. 100219. https://doi.org/10.1016/j.cosrev.2019.100219
22. Zeng J., Wu, S., Chen, Y., Zeng, R., & Wu, C.Survey of attack graph analysis methods from the perspective of data and knowledge processing // Security and Communication Networks. 2019. Т. 2019. Article ID 2031063, 16 С., 2019. https://doi.org/10.1155/2019/2031063
23. Pappaterra M. J., Flammini F. A review of intelligent cybersecurity with Bayesian Networks //2019 IEEE International Conference on Systems, Man and Cybernetics (SMC). – IEEE, 2019. С. 445-452.
24. Sahu A., Davis K. Structural learning techniques for Bayesian attack graphs in cyber physical power systems //2021 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2021. С. 1-6.
25. Wang P. Yang, L. T., Li, J., Chen, J., & Hu, S. Data fusion in cyber-physical-social systems: State-of-the-art and perspectives // Information Fusion. 2019. Т. 51. С. 42-57.
26. Arzhenovskiy S. V., Bakhteev A. V., Sinyavskaya T. G., Hahonova N. N. Audit risk assessment model. International Journal of Economics and Business Administration. 2019. № 1(7). 74-85.
27. Desai V., Kim J. W., Srivastava R. How do auditors issue going concern opinions? A dynamic model under Bayesian Framework: Evidence from 2004 to 2015. Working paper, 2020. 57 С.
28. Baskerville R. L., Kim J., Stucke C. The Cybersecurity Risk Estimation Engine: A Tool for Possibility Based Risk Analysis //Computers & Security. 2022. С. 102752. https://doi.org/10.1016/j.cose.2022.102752
29. Rohmer J. Uncertainties in conditional probability tables of discrete Bayesian Belief Networks: A comprehensive review // Engineering Applications of Artificial Intelligence. 2020. V. 88. P. 103384. https://doi.org/10.1016/j.engappai. 2019.103384
30. Волкова Е.С., Гисин В.Б. Оценка рисков информационной безопасности на основе теории свидетельств Демпстера-Шефера. В «Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики» , С.И.Козьминых ред., 2020. С. 89-101.
31. Dimuro G. P. Fernández, J., Bedregal, B., Mesiar, R., Sanz, J. A., Lucca, G., Bustince, H. The state-of-art of the generalizations of the Choquet integral: from aggregation and pre-aggregation to ordered directionally monotone functions // Information Fusion. 2020. V. 57. P. 27-43. https://doi.org/10.1016/j.inffus.2019.10.005
32. Information Quality in Information Fusion and Decision Making (E. Bossé, G. L. Rogova, eds). Cham, Springer, 2019 –629 P. https://doi.org/10.1007/978-3-030-03643-0.
33. Wang P. Yang, L. T., Li, J., Chen, J., & Hu, S. Data fusion in cyber-physical-social systems: State-of-the-art and perspectives //Information Fusion. 2019. Т. 51. С. 42-57.

BELIEF AND PLAUSIBILITY MEASURES IN ASSESSING INFORMATION SECURITY RISKS

Elena S. Volkova[8], Vladimir B. Gisin[9]

Abstract

Purpose of the research: *to develop methods for assessing information security risks under uncertainty, to describe the mechanism of propagating belief and plausibility in the attack graph.*

Research method: *application of soft computing techniques, including the combination of Dempster-Shafer evidence theory, integration with respect to non-additive measures of belief and plausibility.*

Research result: *risk assessment methods and methods for assessing expected losses have been developed in the case when risk factors are characterized by high uncertainty and do not allow sufficiently justified applying*

8 Elena S. Volkova, Ph.D., Associate Professor, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail:evolkova@fa.ru

9 Vladimir B. Gisin, Ph.D., Professor, Financial University under the Government of the Russian Federation, Moscow, Russia, E-mail:vgisin@fa.ru

objective (probabilistic) assessment methods. The initial information is the upper and lower estimates of the probability of risk realization. Using the methods of the Dempster-Shafer evidence theory, belief and plausibility measures are built on the attack graph. An approach is described that allows building belief and plausibility measures in the space of attack scenarios based on probabilistic estimates of typical information security events. It is shown how the expected damage (severity) can be estimated by the expectation of damage with respect to to these measures using the Choquet integral.

***Scientific novelty:** a method of propagation belief along the attack graph has been developed. The method is based on an original approach to evaluating logical combinations of evidence given on binary frames and represented by disjunctive normal forms.*

***Keywords:** risk, belief measure, plausibility measure, Choquet integral, evidence theory*

References

1. Popov E., Semyachkov K. Umnye goroda. Monografiya. – M.: YUrajt, 2020. 347 s.
2. Innovations in Cybersecurity Education. Kevin Daimi, Guillermo Francia, eds. Springer 2020. 391 P. https://doi.org/10.1007/978-3-030-50244-7
3. Mamaeva L. N., Bekher V. V. Ugrozy kiberbezopasnosti v cifrovom prostranstve //Vestnik Saratovskogo gosudarstvennogo social'no-ekonomicheskogo universiteta. 2019. № 4 (78). P. 68-70.
4. Gas'kova D. A., Massel' A. G. Tekhnologiya analiza kiberugroz i ocenka riskov narusheniya kiberbezopasnosti kriticheskoj infrastruktury // Voprosy kiberbezopasnosti. 2019. № 2 (30). P. 42-49.
5. Review of cybersecurity risk analysis methods and tools for safety critical industrial control systems. VTT Technical Research Centre of Finland. VTT Research Report. VTT-R-00298-22. 2022. 46 p. https://cris.vtt.fi/en/publications/review-of-cybersecurity-risk-analysis-methods-and-tools-for-safet (last accessed 22.01.2023)
6. Upadhyay D., Sampalli S. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations // Computers & Security. – 2020. v. 89. p. 101666.
7. Kalashnikov A. O., Bugajskij K. A. Model' ocenki bezopasnosti slozhnoj seti (chast' 1) // Voprosy kiberbezopasnosti. 2022. №. 4 (50). P. 26-38. DOI:10.21681/2311-3456-2022-4-26-38
8. Landoll D. The security risk assessment handbook: A complete guide for performing security risk assessments. Boca Raton: CRC Press, 2021. 512 p. https://doi.org/10.1201/9781003090441
9. Petturiti D., Vantaggi B. How to assess coherent beliefs: a comparison of different notions of coherence in Dempster-Shafer theory of evidence // In Reflections on the Foundations of Probability and Statistics: Essays in Honor of Teddy Seidenfeld. Cham: Springer International Publishing, 2022. P. 161-185.
10. Lepskij A. E. Analiz protivorechivosti informacii v teorii funkcij doveriya. CH. 1. Vneshnij konflikt //Problemy upravleniya. 2021. №. 5. P. 3-19.
11. Ivanov V. K., Vinogradova, N. V., Palyuh, B. V., & Sotnikov, A. N. Sovremennye napravleniya razvitiya i oblasti prilozheniya teorii Dempstera-SHafera (obzor) // Iskusstvennyj intellekt i prinyatie reshenij. 2018. №. 4. P. 32-42.
12. Naik N., Jenkins P., Kerby B., Sloane J., Yang L. Fuzzy logic aided intelligent threat detection in cisco adaptive security appliance 5500 series firewalls. In 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). – IEEE, 2018. p. 1-8.
13. Guzairov M. B. Vul'fin A. M., Kartak V. M., Kirillova, A. D., Mironov K. V. Sravnitel'nyj analiz algoritmov kognitivnogo modelirovaniya pri ocenke riskov informacionnoj bezopasnosti // Trudy Instituta sistemnogo analiza Rossijskoj akademii nauk. 2019. № 4 (69). P. 62-69. DOI: 10.14357/20790279190408
14. Kalashnikov A. O., Bugajskij K. A. Model' ocenki bezopasnosti slozhnoj seti (chast' 2) // Voprosy kiberbezopasnosti. 2022. № 5 (50). P. 47-60. DOI:10.21681/2311-3456-2022-5-47-60
15. Kaneman D., Siboni O., Sanstejn K.R. Shum. M.: AST, 2021. 590 P.
16. Bruine de Bruin W., Carman K. G. Measuring subjective probabilities: The effect of response mode on the use of focal responses, validity, and respondents' evaluations //Risk Analysis. 2018. № 10 (38). P. 2128-2143. DOI: 10.1111/risa.13138
17. Wilson R. S., Zwickle A., Walpole H. Developing a broadly applicable measure of risk perception //Risk Analysis. 2019. № 4 (39). P. 777-791.
18. Zhang, Z., Jiang, C. Evidence-theory-based structural reliability analysis with epistemic uncertainty: a review. Struct Multidisc Optim 63, 2935–2953 (2021). https://doi.org/10.1007/s00158-021-02863-w
19. Jiroušek R., Kratochvíl V. On subjective expected value under ambiguity // International Journal of Approximate Reasoning. 2020. V. 127. P. 70-82. https://doi.org/10.1016/j.ijar.2020.09.002
20. Dimuro G. P. Fernández, J., Bedregal, B., Mesiar, R., Sanz, J. A., Lucca, G., Bustince, H. The state-of-art of the generalizations of the Choquet integral: from aggregation and pre-aggregation to ordered directionally monotone functions // Information Fusion. 2020. V. 57. P. 27-43. https://doi.org/10.1016/j.inffus.2019.10.005
21. Lallie H. S., Debattista K., Bal J. A review of attack graph and attack tree visual syntax in cyber security //Computer Science Review. 2020. V. 35. P. 100219. https://doi.org/10.1016/j.cosrev.2019.100219
22. Zeng J., Wu, S., Chen, Y., Zeng, R., & Wu, C.Survey of attack graph analysis methods from the perspective of data and knowledge processing // Security and Communication Networks. 2019. V. 2019. Article ID 2031063, 16 P., 2019. https://doi.org/10.1155/2019/2031063
23. Pappaterra M. J., Flammini F. A review of intelligent cybersecurity with Bayesian Networks //2019 IEEE International Conference on Systems, Man and Cybernetics (SMC). – IEEE, 2019. – P. 445-452.
24. Sahu A., Davis K. Structural learning techniques for Bayesian attack graphs in cyber physical power systems //2021 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2021. C. 1-6.

25. Wang P. Yang, L. T., Li, J., Chen, J., & Hu, S. Data fusion in cyber-physical-social systems: State-of-the-art and perspectives // Information Fusion. 2019. V. 51. P. 42-57.
26. Arzhenovskiy S. V., Bakhteev A. V., Sinyavskaya T. G., Hahonova N. N. Audit risk assessment model. International Journal of Economics and Business Administration. 2019. № 1(7). 74-85.
27. Desai V., Kim J. W., Srivastava R. How do auditors issue going concern opinions? A dynamic model under Bayesian Framework: Evidence from 2004 to 2015. Working paper, 2020. 57 P.
28. Baskerville R. L., Kim J., Stucke C. The Cybersecurity Risk Estimation Engine: A Tool for Possibility Based Risk Analysis //Computers & Security. 2022. P. 102752. https://doi.org/10.1016/j.cose.2022.102752
29. Rohmer J. Uncertainties in conditional probability tables of discrete Bayesian Belief Networks: A comprehensive review // Engineering Applications of Artificial Intelligence. 2020. V. 88. P. 103384. https://doi.org/10.1016/j.engappai. 2019.103384
30. Volkova E.S., Gisin V.B. Ocenka riskov informacionnoj bezopasnosti na osnove teorii svidetel'stv Dempstera-SHefera. In «Informacionnaya bezopasnost' finansovo-kreditnyh organizacij v usloviyah cifrovoj transformacii ekonomiki», S.I.Koz'minyh red., 2020. P. 89-101.
31. Dimuro G. P. Fernández, J., Bedregal, B., Mesiar, R., Sanz, J. A., Lucca, G., Bustince, H. The state-of-art of the generalizations of the Choquet integral: from aggregation and pre-aggregation to ordered directionally monotone functions // Information Fusion. 2020. V. 57. P. 27-43. https://doi.org/10.1016/j.inffus.2019.10.005
32. Information Quality in Information Fusion and Decision Making (E. Bossé, G. L. Rogova, eds). Cham, Springer, 2019 –629 p. https://doi.org/10.1007/978-3-030-03643-0.
33. Wang P. Yang, L. T., Li, J., Chen, J., & Hu, S. Data fusion in cyber-physical-social systems: State-of-the-art and perspectives //Information Fusion. – 2019. – V. 51. – P. 42-57.